BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

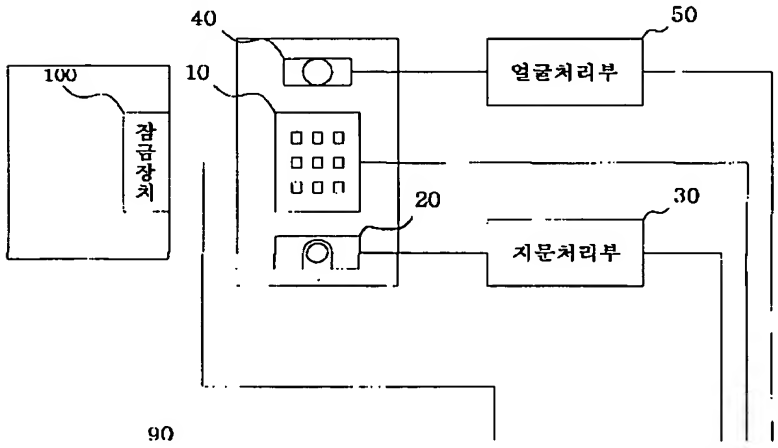
KOREAN PATENT ABSTRACTS (KR)

Document Code:A
(11) Publication No.1020010007874 (43) Publication.Date. 20010205
(21) Application No.1020000060312 (22) Application Date. 20001013
(51) IPC Code:
E05B 49/00

(71) Applicant:
CHOI, HYUNG SUN
(72) Inventor:
CHOI, HYUNG SUN
(30) Priority:

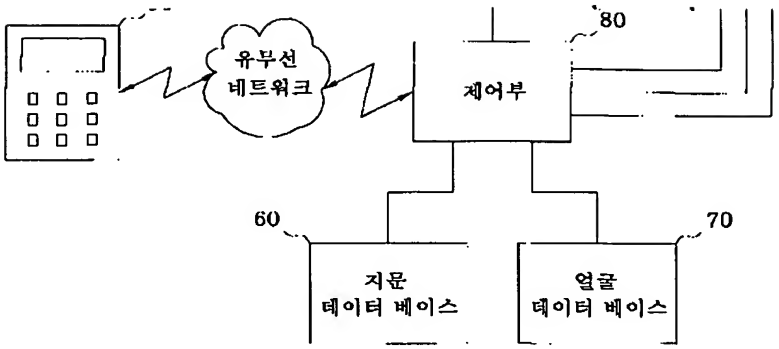
(54) Title of Invention
SYSTEM AND METHOD FOR CONTROLLING ENTRANCE AND EXIT BY USING FINGERPRINT IDENTIFICATION AND FACE IDENTIFICATION

Representative drawing



(57) Abstract:

PURPOSE: A system and a method for controlling entrance and exit by using fingerprint identification and face identification are provided to improve the degree of



accuracy and security.

CONSTITUTION: A system for controlling entrance and exit by using fingerprint identification and face identification includes a key pad(10) receiving input of a secret number from a person, a fingerprint identification sensor(20) for identifying the fingerprint of the person, a fingerprint processing part(30) extracting a characteristic from the fingerprint identification sensor for making data, a camera (40) identifying a face of the person, a face processing part (50) extracting a characteristic from the face image signal identified through the camera for making data, a fingerprint database(60) storing IDs of persons allowed to entrance and exit and the corresponding fingerprint data, a face database (70) storing the IDs shared with the fingerprint database and the corresponding face data, a network contacting part contacting with the external terminal through a wire and wireless network, and a control part(80) opening and shutting a locking device of a gate.

if display of image is failed, press (F5)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2001-0007874
E05B 49/00		(43) 공개일자	2001년02월05일
(21) 출원번호	10-2000-0060312		
(22) 출원일자	2000년10월13일		
---	---
(71) 출원인	최형선 대한민국 121-140 서울 마포구 신정동 28-2 성진빌딩 5 6층
(72) 발명자	최형선 대한민국 121-140 서울 마포구 신정동 28-2 성진빌딩 5 6층
(74) 대리인	특허법인 원전 임석재 특허법인 원전 윤우성
---	---
(77) 심사청구	있음

(54) 출원명 지문인식 및 얼굴인식을 이용한 출입통제시스템 및 그 방법

요약

본 발명은 지문인식 및 얼굴인식을 이용한 출입통제시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 출입이 허가된 사람들의 지문데이터와 얼굴데이터를 저장한 데이터베이스와 카메라 및 지문인식센서를 구비하여, 지문과 얼굴이 인증된 출입자에게만 출입을 허가하고, 인증되지 않은 출입자의 경우에는 지문과 얼굴 영상을 저장하여 보안성을 보다 향상시킨 출입통제시스템 및 그 방법에 관한 것이다.

본 발명에서의 출입통제시스템은 비밀번호인증을 위한 키패드(10), 지문인증을 위한 지문인식센서(20) 및 지문처리부(30), 얼굴인증을 위한 카메라(40) 및 얼굴처리부(50), 등록된 지문데이터가 저장된 지문데이터베이스(60) 및 등록된 얼굴데이터가 저장된 얼굴데이터베이스(70)로 이루어진다.

본 발명에서의 출입통제방법은 비밀번호인증단계(S100), 지문인증단계(S200), 얼굴인증단계(S300) 및 장금장치해제단계(S400)로 이루어지는데, 인증되지 않는 경우에는 지문 또는 얼굴 영상을 저장하고, 유무선 네트워크를 통해 관리자 단말기로 얼굴 영상을 전송하여 관리자로부터 인증신호를 받아서 인증할 수 있다.

대표도

도1

색인어

지문인식, 얼굴인식, 출입통제시스템, 출입통제방법, 보안, 인증.

명세서

도면의 간단한 설명

도 1은 본 발명에 의한 출입통제시스템을 개략적으로 도시한 구성도,

도 2는 본 발명에 의한 출입통제방법의 흐름을 개략적으로 도시한 흐름도,

도 3은 본 발명에 의한 출입통제방법의 흐름을 상세히 도시한 흐름도,

도 4는 본 발명에 의한 출입통제방법에 있어서 인증단계의 다른 실시예를 도시한 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 지문인식 및 얼굴인식을 이용한 출입통제시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 출입이 허가된 사람들의 지문데이터와 얼굴데이터를 저장한 데이터베이스와 카메라 및 지문인식센서를 구비하여, 지문인증 및 얼굴인증의 단계를 거쳐 인증된 출입자에게만 출입을 허가하고, 인증되지 않은 출입자의 경우에는 지문과 얼굴 영상을 저장하도록 하여 보안성을 보다 향상시킨 출입통제시스템 및 그 방법에 관한 것이다.

종래의 출입통제시스템 및 그 방법을 살펴보면, 보안이 요구되는 연구소나 사무실의 경우에 비밀번호를 입력하도록 하여 출입 허가 여부를 결정하는 것이 보편적이다. 그러나, 이러한 경우에 비밀번호가 누출될 우려가 있다는 문제가 있다.

따라서, 근래에는 출입자의 고유한 특징인 지문이나 얼굴 등을 이용하여 출입 허가 여부를 결정하고자 하는 연구가 활발히 진행되고 있으며, 지문 인식의 경우에는 이미 그 실용화 단계에 까지 와 있다고 할 수 있다.

그러나, 지문인식으로 100% 완벽하게 출입자를 선별할 수는 없는 것이어서, 정당한 출입자를 거절하거나 등록되지 않은 출입자에게 출입을 허가하는 등의 오류를 범할 가능성이 있다. 얼굴인식은 정확도를 높이면 높일수록 데이터의 양이 증가하게 되고, 이를 인증하기 위해 데이터를 비교하는 과정에서 상당한 시간이 소요되는 문제가 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제를 해결하기 위해 안출된 것으로, 비밀번호, 지문인식 및 얼굴인식을 효과적으로 연동시켜서 인증판단의 정확도를 높이고, 인증되지 않은 출입자의 경우에는 지문 및 얼굴 영상을 저장함으로써, 보안성이 보다 향상된 출입통제시스템 및 그 방법을 제공하는 것을 그 목적으로 한다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위하여, 본 발명에 의한 출입통제시스템은 출입자로부터 비밀번호를 입력받는 키패드와, 상기 출입자의 지문을 인식하기 위한 지문인식센서와, 상기 지문입력센서를 통해 인식된 지문으로부터 특징을 추출하여 데이터화하는 지문처리부와, 상기 출입자의 얼굴을 인식하기 위한 카메라와, 상기 카메라를 통해 인식된 얼굴 영상신호로부터 특징을 추출하여 데이터화하는 얼굴처리부와, 출입이 허가된 사람들의 ID와 이에 해당하는 지문데이터가 저장된 지문데이터베이스와, 상기 지문데이터베이스와 공유하는 ID와 이에 해당하는 사람의 얼굴데이터가 저장된 얼굴데이터베이스와, 유무선 네트워크를 통해 외부 단말기와 접속할 수 있는 네트워크접속부와, 상기 키패드를 통해 입력되는 비밀번호를 인증하고, 비밀번호가 인증되면 상기 지문처리부로부터 입력되는 상기 출입자의 지문데이터를 상기 지문데이터베이스에 저장된 지문데이터와 비교검색하여 인증하고, 지문이 인증되면 상기 얼굴처리부로부터 입력되는 상기 출입자의 얼굴데이터를 상기 얼굴데이터베이스의 상기 지문이 인증된 ID의 해당 얼굴데이터와 비교하여 인증하거나, 상기 출입자의 얼굴 영상을 상기 네트워크접속부를 이용하여 유무선 네트워크를 통해 관리자의 단말기로 전송하고 상기 관리자로부터 인증신호를 입력받아서 인증하여, 출입문의 잠금장치를 개폐하는 제어부를 포함하여 이루어지는 것을 특징으로 한다.

여기서, 상기 지문인식센서는 상기 키패드의 각 버튼에 설치되어, 상기 출입자가 비밀번호를 입력하기 위해 상기 버튼을 누름과 동시에 상기 출입자의 지문을 인식하도록 할 수 있다.

상기 출입통제시스템을 이용한 본 발명에 의한 출입통제방법은 출입자가 키패드를 통해 비밀번호를 입력하면, 미리 저장된 비밀번호와 일치하는지 여부를 판단하는 비밀번호인증단계와, 상기 출입자가 입력한 비밀번호와 미리 저장된 비밀번호가 일치하는 경우에, 상기 출입자의 지문을 인식하는 지문인식단계와, 상기 지문인식단계에서 인식된 지문데이터와 지문데이터베이스에 저장된 지문데이터를 비교하여 상기 출입자의 지문이 등록된 지문인지 여부를 판단하는 지문인증단계와, 상기 지문인증단계에서 상기 출입자의 지문이 등록된 지문인 경우에, 카메라를 통해 상기 출입자의 얼굴을 인식하는 얼굴인식단계와, 얼굴데이터베이스로부터 상기 지문인증단계에서 파악된 출입자에 해당하는 얼굴데이터를 검출하고, 이를 상기 얼굴인식단계에서 인식된 얼굴데이터와 비교하여 등록된 얼굴인지 여부를 판단하는 얼굴인증단계와, 상기 얼굴인증단계에서 등록된 얼굴로 판단된 경우에, 출입문의 잠금장치를 해제하는 잠금해제단계로 이루어지는 것을 특징으로 한다.

여기서, 상기 지문인증단계 또는 얼굴인증단계에서 상기 지문 또는 얼굴이 등록된 지문 또는 얼굴이 아닌 경우에는, 상기 지문인식단계 또는 얼굴인식단계에서 인식된 상기 출입자의 지문 또는 얼굴 영상을 저장하는 영상저장단계를 더 구비하여 이루어지는 것을 다른 특징으로 한다.

또한, 상기 비밀번호인증단계나 지문인증단계 또는 얼굴인증단계에서, 상기 출입자가 인증받지 못한 경우에 상기 카메라를 통해 입력된 상기 출입자의 얼굴 영상을 유무선 네트워크를 관리자의 단말기로 전송하고, 상기 관리자로부터 출입허가여부의 인증신호를 입력받아서 인증할 수 있는 것을 또 다른 특징으로 한다.

이하 첨부된 도면을 참조하여 본 발명에 대하여 보다 상세하게 설명하겠다.

도 1은 본 발명에 의한 출입통제시스템의 구성을 개략적으로 도시한 구성도이다.

도 1에 도시한 바와 같이, 본 발명에 의한 출입통제시스템은, 출입문측에 설치되어 비밀번호를 입력받는 키패드(10)와, 출입자의 지문을 인식하는 지문인식센서(20)와, 상기 지문에서 특징을 추출하여 데이터화하는 지문처리부(30)와, 상기 출입자의 얼굴 영상을 인식하는 카메라(40)와, 상기 카메라를 통해 인식된 얼굴 영상에서 특징을 추출하여 데이터화하는 얼굴처리부(50)와, 출입이 허가된 사람들의 지문데이터가 저장된 지문데이터베이스(60)와, 출입이 허가된 사람들의 얼굴데이터가 저장된 얼굴데이터베이스(70)와, 상기 키패드(10)로부터 입력되는 비밀번호를 인증하고, 상기 지문처리부(30)로부터 입력되는 지문데이터를 상기 지문데이터베이스(60)를 참조하여 인증하고, 상기 얼굴처리부(50)로부터 입력되는 얼굴데이터를 상기 얼굴데이터베이스(70)를 참조하여 인증하고, 최종적으로 모든 인증단계를 통과하여 출입이 허가된 사람으로 판단되면 출입문의 잠금장치(100)를 해제하는 제어부(80)를 포함하여 이루어진다.

또한, 상기 제어부는 유무선 네트워크를 통해 관리자의 단말기(90)에 접속하여, 상기 카메라(40)를 통해 인식되는 출입자의 얼굴 영상을 상기 관리자의 단말기(90)로 전송한다. 이때, 상기 관리자는 단말기(90)를 통해 출입자를 확인하고, 인증신호를 다시 상기 제어부(80)로 전송하여, 원거리에서 출입을 통제할 수 있게 된다.

여기서, 상기 지문인식센서(20)는 상기 키패드(10)의 각 버튼에 설치할 수도 있다. 이러한 경우에는 출입자가 비밀번호를 입력하기 위해 버튼을 누름과 동시에 상기 출입자의 지문을 인식하고, 비밀번호의 자릿수만큼 입력된 지문에 대하여 상기 지문처리부(30)에서 특징을 추출하도록 하여 보다 정확도를 높일 수 있다.

상기 비밀통제시스템을 이용한 출입통제방법의 흐름은 도 2에 개략적으로 도시되어 있다.

도 2에 도시된 바와 같이, 본 발명에 의한 출입통제방법은 비밀번호인증단계(S100), 지문인증단계(S200), 얼굴인증단계(S300) 및 잠금장치해제단계(S400)로 이루어 진다. 즉, 출입자로부터 비밀번호를 확인하고, 비밀번호가 인증되면 지문을 입력받아서 등록된 지문인지를 판단하고, 지문이 인증되면 얼굴 영상을 입력받아서 등록된 얼굴인지를 판단하게 된다. 이와 같이, 본 발명에 의한 출입통제방법은 비밀번호, 지문 및 얼굴의 세가지 단계를 통해 출입자를 인증함으로써 보다 높은 보안성을 제공한다.

도 3은 본 발명에 의한 출입통제방법을 보다 상세하게 설명하기 위한 흐름도이다.

도 3에 도시된 바와 같이, 본 발명에 의한 출입통제방법은, 출입자가 키패드를 이용하여 비밀번호를 입력하는 단계(S11)와, 상기 비밀번호가 등록된 비밀번호인지 여부를 제어부가 판단하는 단계(S120)와, 비밀번호가 인증되면 지문인식센서를 통해 상기 출입자의 지문을 인식하는 단계(S210)와, 상기 지문으로부터 특징으로 추출하여 데이터화하고, 지문데이터베이스를 검색하여 이와 동일한 지문을 찾는 단계(S220)와, 출입자의 지문이 지문데이터베이스에 등록된 지문인지를 판단하는 단계(S230)와, 지문이 인증되면 카메라를 통해 출입자의 얼굴 영상을 입력받는 단계(S310)와, 상기 얼굴 영상으로부터 특징을 추출하여 데이터화하고, 상기 지문인증시에 동일한 지문으로 판단된 사람의 얼굴데이터를 얼굴데이터베이스에서 검출하여 이를 상기 카메라를 통해 입력된 얼굴데이터와 비교하는 단계(S330)와, 동일한 얼굴인지 여부를 판단하는 단계(S330)와, 얼굴까지 인증되면 출입문의 잠금장치를 해제하는 단계(S400)를 포함하여 이루어진다.

이때, 상기 등록된 지문인지 여부를 판단하는 단계(S230) 또는 상기 동일한 얼굴인지 여부를 판단하는 단계(S330)에서 등록된 지문 또느 얼굴이 아닌것으로 판단되는 경우에는 인식된 지문을 저장하는 단계(S510)와 비밀번호, 지문, 얼굴의 각 인증과정에서 등록된 사람이 아니라고 판단되는 경우에는 카메라를 통해 인식되는 출입자의 얼굴 영상을 저장하는 단계(S500)를 더 포함하여 이루어진다.

여기서, 지문데이터베이스와 얼굴데이터베이스는 각 지문데이터 또는 얼굴데이터에 해당하는 사람의 ID를 공유하고, 얼굴인증단계에서는 지문인증단계에서 인증된 사람의 ID에 해당하는 얼굴데이터를 검출하여 카메라로부터 입력되는 얼굴데이터와 비교하도록 하여 얼굴인식에 소요되는 시간을 단축시킨다.

도 4는 본 발명에 의한 출입통제방법에 있어서 인증단계의 다른 실시예를 도시한 흐름도이다.

도 4에 도시된 바와 같이, 출입자의 얼굴을 인증하는 단계는, 카메라를 통해 출입자의 얼굴 영상을 입력받는 단계(S600)와, 제어부가 유무선 네트워크를 통해 관리자의 단말기에 접속하는 단계(S610)와, 상기 관리자의 단말기로 상기 얼굴 영상을 전송하는 단계(S620)와, 상기 관리자로부터 인증신호를 입력받는 단계(S630)와, 상기 신호를 판별하여 인증여부를 결정하는 단계(S640)와, 상기 관리자에 의해 인증되면 출입문의 잠금장치를 해제하는 단계(S650)와, 인증되지 않으면 상기 얼굴 영상을 저장하는 단계(S660)로 이루어진다.

도 4에서는 얼굴인증단계를 예로서 설명하였으나, 키패드에 별도의 버튼을 설치하여 출입자가 원하는 경우에 직접 관리자와 유무선 네트워크를 통해 접속할 수 있도록 할 수도 있으며, 얼굴인증단계 뿐 아니라 비밀번호인증단계 또는 지문인증단계에서 인증되지 않는 경우에도 유무선 네트워크를 통해 관리자에게 직접 인증받도록 할 수 있다.

발명의 효과

본 발명에 의한 출입통제시스템 및 그 방법을 사용하는 경우에는, 비밀번호의 인증, 지문의 인증, 얼굴의 인증이라는 세가지 단계의 인증을 거쳐 출입인가 여부를 결정하고, 인증되지 않는 경우에는 출입자의 지문 또는 얼굴 영상을 저장함으로써, 보다 높은 보안성을 유지할 수 있다는 효과를 얻을 수 있다.

또한, 지문데이터베이스와 얼굴데이터베이스는 각 지문데이터 또는 얼굴데이터에 해당하는 사람의 ID를 공유하고, 지문인증단계에서 인증된 사람의 ID에 해당하는 얼굴데이터를 검출하여 카메라로부터 입력되는 얼굴데이터와 비교함으로써, 얼굴인식에서 소요되는 시간을 상당히 단축시키는 효과를 얻을 수 있다.

또한, 유무선 네트워크를 통해 관리자의 단말기에 접속하여 출입자의 얼굴 영상을 전송하고, 상기 관리자로부터 인증신호를 입력받음으로써, 관리자는 원거리에서도 출입을 통제할 수 있으며, 등록된 사람이 아닐지라도 관리자의 부재중에 출입할 필요가 있는 사람에 대하여 출입을 허가해 줄 수 있게 되고, 인증과정에서 오류가 발생하거나, 손가락에 상처를 입어서 지문인증을 받을 수 없는 경우에도 관리자로부터 인증을 받아서 출입할 수 있도록 하는 효과를 얻을 수 있다.

(57) 청구의 범위

청구항 1.

지문인식 및 얼굴인식을 이용한 출입통제시스템에 있어서,

출입자로부터 비밀번호를 입력받는 키패드(10)와;

상기 출입자의 지문을 인식하기 위한 지문인식센서(20)와;

상기 지문입력센서를 통해 인식된 지문으로부터 특징을 추출하여 데이터화하는 지문처리부(30)와;

상기 출입자의 얼굴을 인식하기 위한 카메라(40)와;

상기 카메라를 통해 인식된 얼굴 영상신호로부터 특징을 추출하여 데이터화하는 얼굴처리부(50)와;

출입이 허가된 사람들의 ID와 이에 해당하는 지문데이터가 저장된 지문데이터베이스(60)와;

상기 지문데이터베이스와 공유하는 ID와 이에 해당하는 사람의 얼굴데이터가 저장된 얼굴데이터베이스(70)와;

유무선 네트워크를 통해 외부 단말기와 접속할 수 있는 네트워크접속부와;

상기 키패드를 통해 입력되는 비밀번호를 인증하고, 비밀번호가 인증되면 상기 지문처리부로부터 입력되는 상기 출입자의 지문데이터를 상기 지문데이터베이스에 저장된 지문데이터와 비교검색하여 인증하고, 지문이 인증되면 상기 얼굴처리부로부터 입력되는 상기 출입자의 얼굴데이터를 상기 얼굴데이터베이스의 상기 지문이 인증된 ID의 해당 얼굴데이터와 비교하여 인증하거나, 상기 출입자의 얼굴 영상을 상기 네트워크접속부를 이용하여 유무선 네트워크를 통해 관리자의 단말기로 전송하고 상기 관리자로부터 인증신호를 입력받아서 인증하여, 출입문의 잠금장치를 개폐하는 제어부(80)를 포함하여 이루어지는 것을 특징으로 하는 출입통제시스템.

청구항 2.

제 1 항에 있어서,

상기 지문인식센서(20)는 상기 키패드(10)의 각 버튼에 설치되어, 상기 출입자가 비밀번호를 입력하기 위해 상기 버튼을 누름과 동시에 상기 출입자의 지문을 인식하도록 설치되어 있는 것을 특징으로 하는 출입통제시스템.

청구항 3.
제 1 항 또는 제 2 항에 의한 출입통제시스템을 이용한 출입 통제 방법에 있어서,

출입자가 키패드를 통해 비밀번호를 입력하면, 미리 저장된 비밀번호와 일치하는지 여부를 판단하는 비밀번호인증단계와;

상기 출입자가 입력한 비밀번호와 미리 저장된 비밀번호가 일치하는 경우에, 상기 출입자의 지문을 인식하는 지문인식단계와;

상기 지문인식단계에서 인식된 지문데이터와 지문데이터베이스에 저장된 지문데이터를 비교하여 상기 출입자의 지문이 등록된 지문인지 여부를 판단하는 지문인증단계와;

상기 지문인증단계에서 상기 출입자의 지문이 등록된 지문인 경우에, 카메라를 통해 상기 출입자의 얼굴을 인식하는 얼굴인식단계와;

얼굴데이터베이스로부터 상기 지문인증단계에서 파악된 출입자에 해당하는 얼굴데이터를 검출하고, 이를 상기 얼굴인식단계에서 인식된 얼굴데이터와 비교하여 등록된 얼굴인지 여부를 판단하는 얼굴인증단계와;

상기 얼굴인증단계에서 등록된 얼굴로 판단된 경우에, 출입문의 잠금장치를 해제하는 잠금해제단계로 이루어지는 것을 특징으로 하는 출입 통제 방법.

청구항 4.
제 3 항에 있어서,

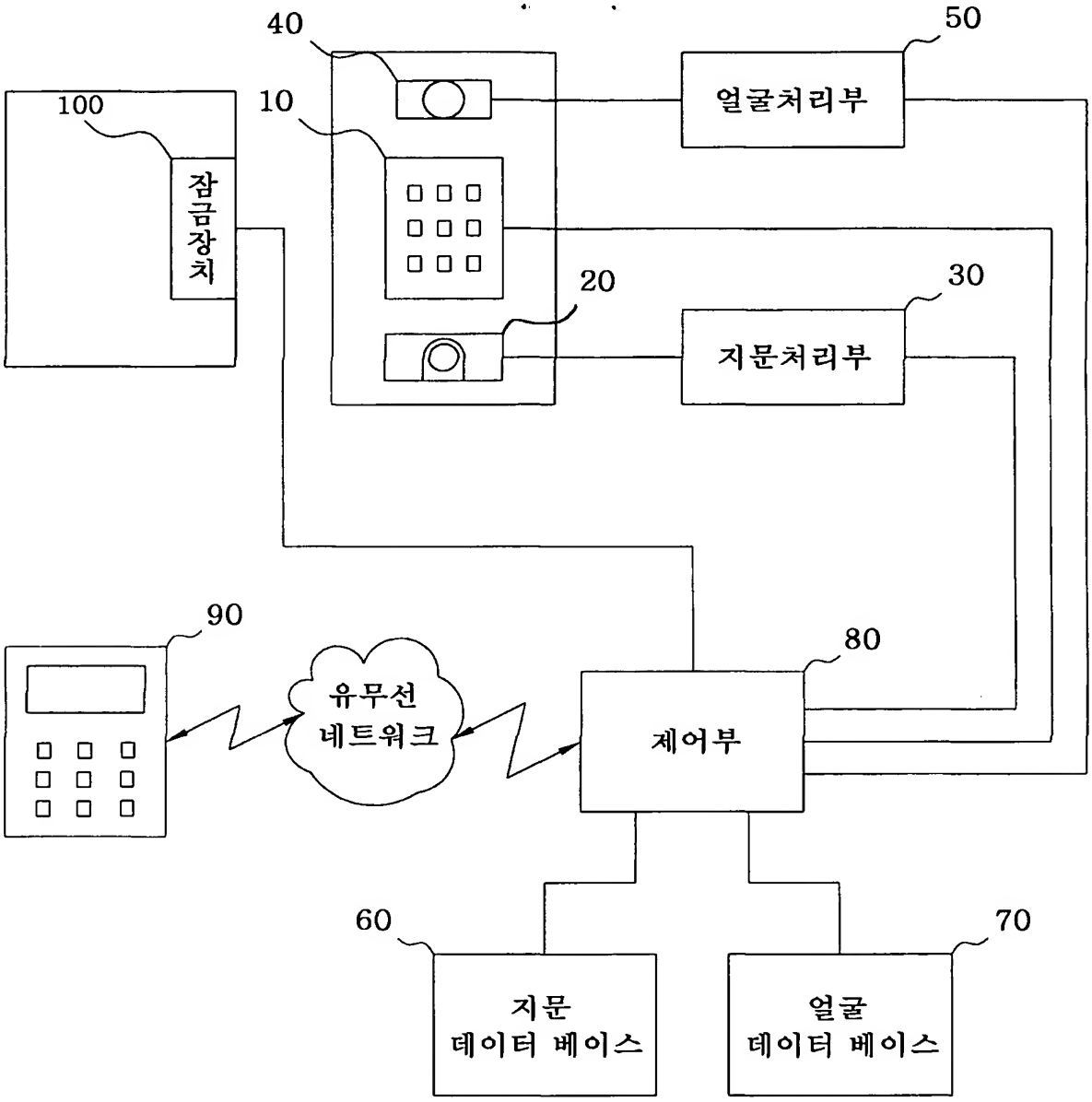
상기 지문인증단계 또는 얼굴인증단계에서 상기 지문 또는 얼굴이 등록된 지문 또는 얼굴이 아닌 경우에는, 상기 지문인식단계 또는 얼굴인식단계에서 인식된 상기 출입자의 지문 또는 얼굴 영상을 저장하는 영상저장단계를 더 구비하여 이루어지는 것을 특징으로 하는 출입 통제 방법.

청구항 5.
제 3 항 또는 제 4 항에 있어서,

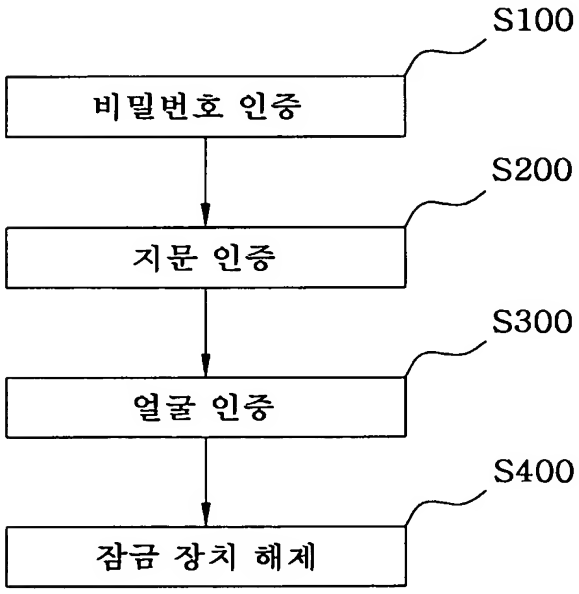
상기 비밀번호인증단계나 지문인증단계 또는 얼굴인증단계에서, 상기 출입자가 인증받지 못한 경우에 상기 카메라를 통해 입력된 상기 출입자의 얼굴 영상을 유무선 네트워크를 관리자의 단말기로 전송하고, 상기 관리자로부터 출입허가여부의 인증신호를 입력받아서 인증할 수 있는 것을 특징으로 하는 출입 통제 방법.

도면

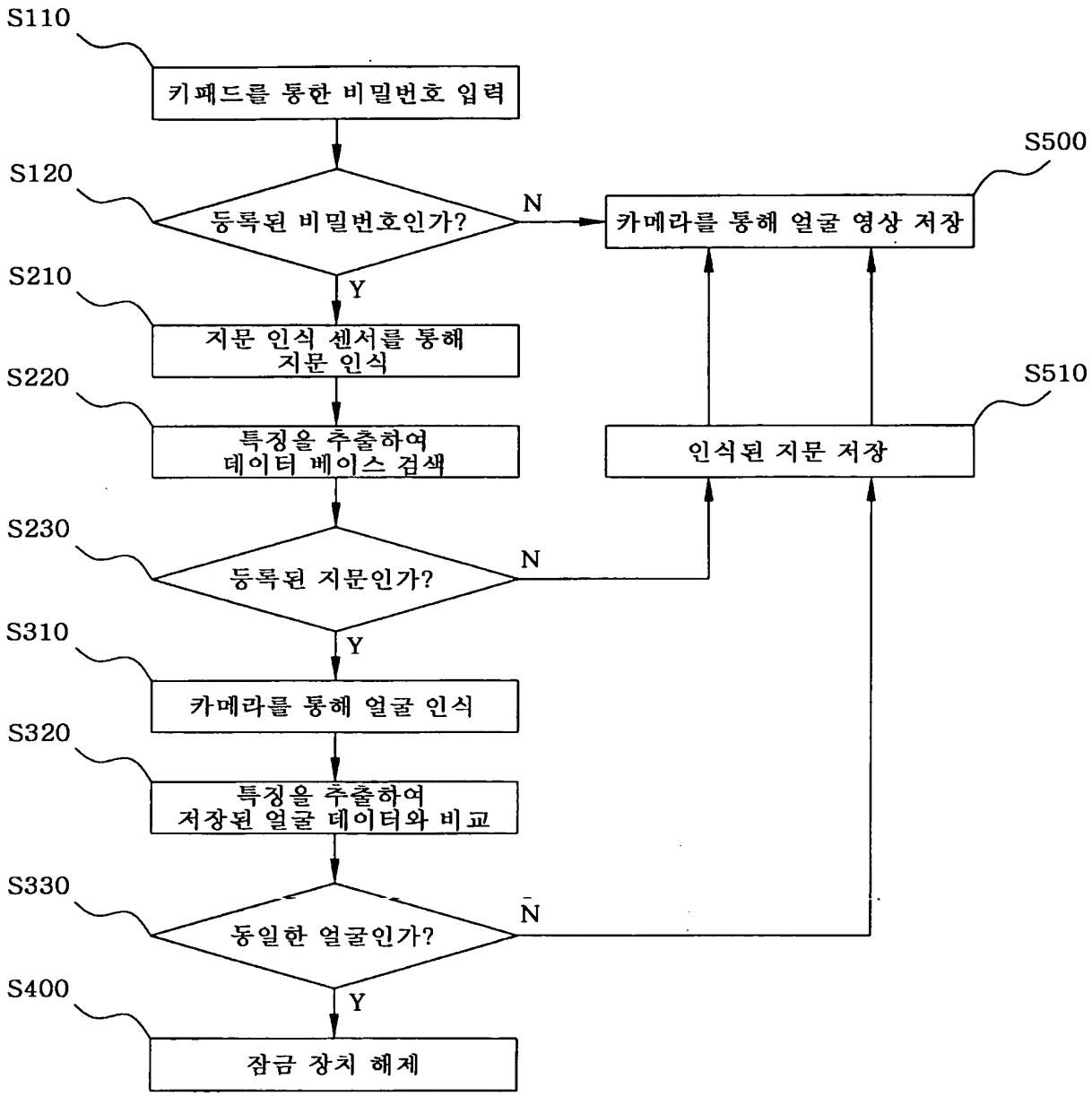
도면 1


40
50
100
10
얼굴처리부
잠금장치
20
30
지문처리부
90
80
유무선
네트워크
제어부
60
70
지문
데이터 베이스
얼굴
데이터 베이스

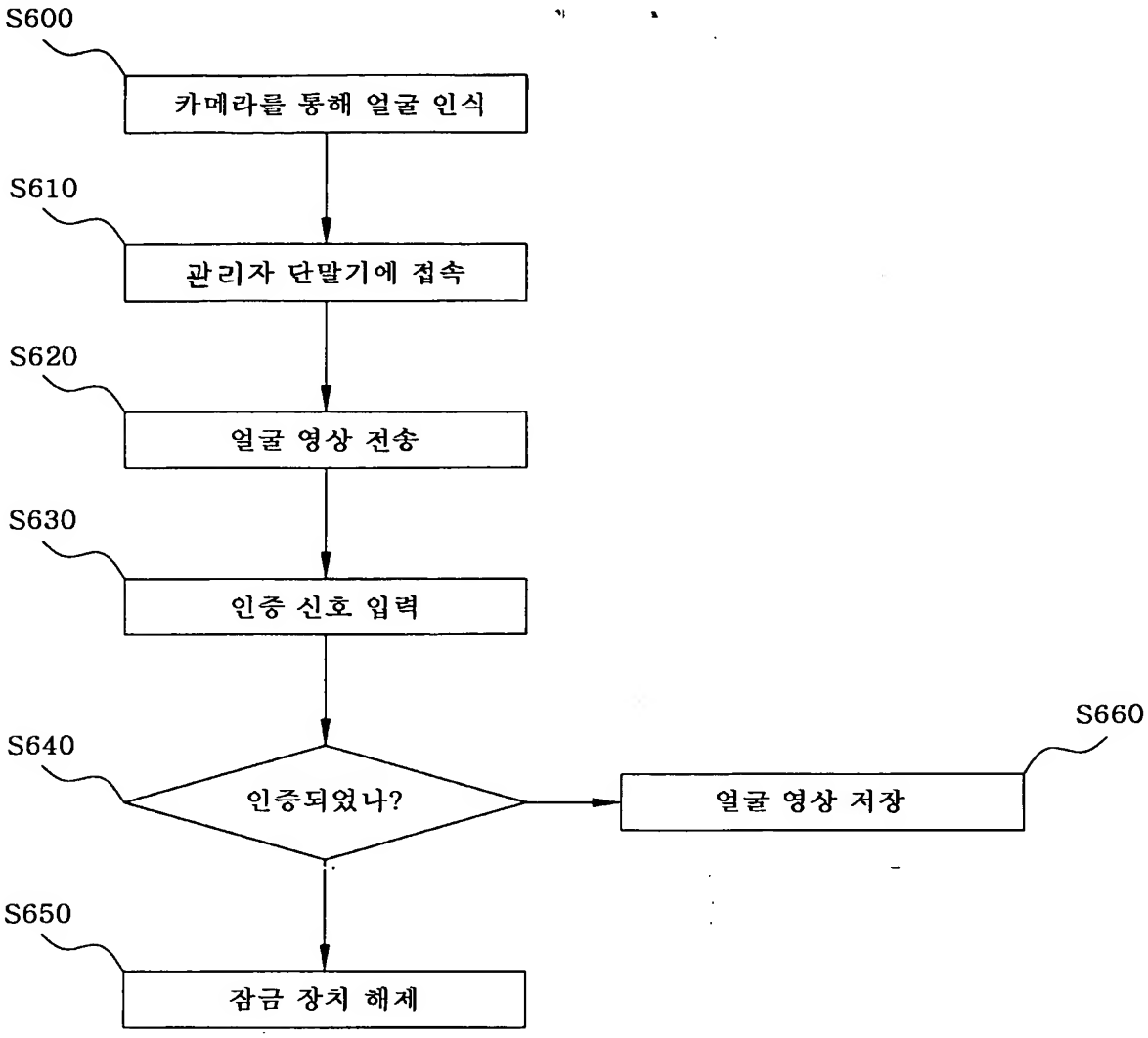
도면 2


S100
비밀번호 인증
S200
지문 인증
S300
얼굴 인증
S400
잠금 장치 해제

도면 3


S110
키패드를 통한 비밀번호 입력
S120
등록된 비밀번호인가?
N
S500
카메라를 통해 얼굴 영상 저장
Y
S210
지문 인식 센서를 통해 지문 인식
S220
특징을 추출하여 데이터 베이스 검색
S510
인식된 지문 저장
S230
등록된 지문인가?
N
Y
S310
카메라를 통해 얼굴 인식
S320
특징을 추출하여 저장된 얼굴 데이터와 비교
S330
동일한 얼굴인가?
N
Y
S400
잠금 장치 해제

도면 4


S600
카메라를 통해 얼굴 인식
S610
관리자 단말기에 접속
S620
얼굴 영상 전송
S630
인증 신호 입력
S640
인증되었나?
S660
얼굴 영상 저장
S650
잠금 장치 해제